E-Voting Solution for Romanian Parliament

Liviu Dunaev
Daniel Platon
MA Student in Economic Informatics
liviu.dunaev@softnet.ro
daniel.platon@softnet.ro

Every year hundreds of millions of people vote in a variety of settings in many countries around the world. People vote in public elections to choose government leaders and also in private elections to determine the course of action for groups that people are organized in such as non-governmental organizations, unions, associations and corporations (shareholders). Voting is a widely spread, rather democratic, way of making decisions. More and more governments and private organizations realize that the use of new technologies such as the Internet can have beneficial impacts on elections - i.e. higher voter turnout and lower costs of conducting elections. The rules governing elections tend to be highly specialized to meet the specific needs of each type of organization. Most elections, however, require integrity, privacy and authentication.

A reliable and failsafe e-voting software technology guarantees the integrity, privacy and authentication of all voters and their individual votes during the election process. To protect the integrity of the institution holding the election, the software should employs sophisticated algorithms to authenticate all voters and thereby ensures that only those individuals who are authorized to vote can actually cast a ballot. It also prevents voters from voting more than once in a given election. To protect the voter, the software should employs proven privacy protection technology to keep all votes anonymous to all parties involved in the process. The solution should consist of modules that can be embedded on private e-voting systems and e-government platforms.

The Problem

As of January 2002 the Internet had more than 125 million unique domains, 36 million Web servers, approximately one billion Web pages and hundreds of millions of users around the globe. While its inherent openness has made the rapid and universal adoption of the Internet possible, it has also led to wide abuse: internet fraud, invasion of privacy, and identity theft.

The 2001 Computer Crime and Security Survey, published by the Computer Security Institute in collaboration with the FBI, revealed that 85% of companies and government agencies surveyed had detected computer security breaches within the last 12 months. From unannounced information gathering by Web sites, to invasion of corporate networks by hackers, the Internet has become the medium of choice for those who want to diminish the privacy, safety and security of others.

The right to privacy is something many individuals take for granted. But as computers increasingly play a bigger role in people's lives, privacy rights are changing and are being called into question. There are many situations, however, where individuals, corporations and governments have a vital interest in keeping certain online transactions private and secure.

The goal of CyberVote is to develop and demonstrate the first highly secure cyber-voting prototype using mobile and fixed internet technologies. The project will define and implement a CyberVote prototype

embedding an innovative voting protocol relying upon the use of advanced cryptographic tools that will be developed to ensure integrity, privacy and authentication of the voters. The project will also analyze the laws in force in the participating countries.

What is an online voting system?

First of all what is an online voting system?

Elections may be organized in many different ways. *Paper-based elections* make use of paper ballots, while *automated elections* make use of some kind of voting machines which automate the voting and/or tabulation procedures. When these voting machines are computers, we talk about *electronic voting*.

Electronic voting systems may be further divided into offline and online voting systems. In *offline voting* systems the computers used may in essence be viewed as a stand-alone computer. In *online voting* systems the computers used are connected by a (closed or open) network, leading to an essential distinction between clients and servers.

Electronic Democracy (or e-Democracy) systems, which may in turn be viewed as parts of *e-Government* systems, form a broad class of systems related to public services targeted at informing citizens on political issues. Such systems may also cater for online discussions between citizens, possibly involving politicians too. These systems may also include mechanisms for *online polls*, which may be used for conducting informal surveys, without seeking a high level of accuracy of the result. *Online voting* systems are much more formal than online polling systems, because they seek (or should seek) to accurately reflect the voters' preferences.

The California Internet Task Force (The Internet Voting Report[1]) describes *Internet voting* as a voting process that enables voters to cast a secure and secret ballot over the Internet. Two main types of Internet voting systems can be recognized: polling place Internet voting and remote Internet voting.

A *polling place Internet voting system* uses Internet voting computers at traditional polling places staffed by election officials who assist in the authentication of voters before ballots are cast.

A *remote Internet voting system* uses unsupervised Internet voting computers to cast a ballot over the Internet using a computer not necessarily owned and operated by election personnel. CyberVote also extends to voting by Mobile Phone. As far as the legal analysis is concerned, Mobile Phone voting is similar to remote Internet voting and will therefore be treated likewise.

The technical architecture of these two systems may differ substantially, because the technological and security concerns are more daunting in the second system.
The polling place voting system would not require a digital authentication: the authentication can be done physically, similar to traditional or electronic election. After the voter is authenticated, she can cast his/her vote anonymously. The authentication procedure and voting process for polling place Internet voting system would therefore (to a certain extent) not differ substantially from the electronic elections organized today.

The remote Internet voting system would require electronic (for instance digital) authentication: the voter would need to have a personal key (password, digital signature) to distantly identify him/her as a legitimate voter. The authentication is necessary to guarantee the one man, one vote principle. But at the same time, the link between the authenticated voter and the ballot cast must be cut, so as to make it not retraceable. It is clear that a digital authentication procedure requires a highly sophisticated technical solution. The authentication is indeed described as one of the most difficult challenges for an Internet voting system.

The Solution

Taking in concern all presented before, our research project take as target the voting procedures that are taking place in the Romanian Chamber of Deputies.

Firs of all lets see how the things are done now:

All the laws, decisions and motions are adopted by the Chamber of Deputies by vote. The vote of the deputy is personal. It may be open or secret. The Open vote shall be expressed by show of hands, by standing up, by roll-call or by electronic means. The secret vote shall be expressed through voting papers, through balls or through electronic means. On the proposal of the president or of a parliamentary group the Chamber shall decide which voting modality shall be used, except for the case in which the regulation establishes a certain voting procedure.

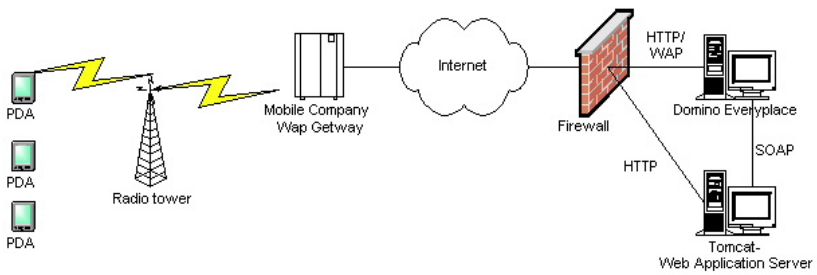
The voting by electronic means shall be done by connecting one of the contacts which represents "Vote for", "Vote against" or "Abstention". The result of the electronic voting shall be displayed on the order of the Chamber's president. In case the Chamber's president, assisted by the two secretaries, shall establish the existence of some faults in the connection of the circuits, he may request the repeating of the electronic voting or its replacing with another voting procedure.

The device allowing the access of the deputy to the electronic means of voting shall be personal. Its utilization by another deputy is prohibited.

Well at least this is the way the law is expressing. But we know that the things are not quite this way. Frauds were made before, frauds will be done again. So to solve the problem, we think that there can be a way to do some improvement of the voting procedures, not only about frauds but also about absentee ballot.

Our proposed system is based on internet voting, and more than this on a cyber voting system for internet terminals and mobile phones. The technology resides in a powerful internet enabled system that will assure that all votes will be expressed by the authorized person and no fraud will be possible. Also it assures a higher presence by the deputies, because it uses a very important device: the mobile phone. This device is very unlikely to be borrowed to somebody else, unlike electronic voting cards.

Figure 1 depicts the architecture of the e-Voting system. The core of the system resides in its administration module that runs on a web application server that can be Tomcat, Websphere, Bea Weblogic, Oracle AS etc. The application is deployed on mobile devices using Lotus Domino Everyplace.



The person in charge with the administration of the system uses the administration module to declare mobile users and to post data about normative papers such as number, date and description. This module is also use to generate statistics about the voting procedures and the papers database, such as the number of laws posted, the voting status. The administrator will submit laws for voting using this module.

To vote, the normal users access the mobile site via their WAP enabled devices (mobile phones, PDAs) where they can see a list of laws submitted to their attention, sorted by their number. Also, they can read a short description of the laws. They have the possibility to choose between three alternatives – Yes, No or Abstention. After they choose one of these, and they confirm their option no further changes of mind are accepted.

The administration module, built using modern web technologies such as XML, XSLT, JSP, servlets, communicates with the mobile web server (Lotus Domino Everyplace) via SOAP. The module sends the data to the web server in order to be accessible to the mobile users. It also receive the response given by the users to the mobile web server and updates the database.

The mobile web server then sends the data to its WAP gateway. The mobile web server ensures the communication's security as well as the user's authentication. Mobile users can only authenticate using their name and password provided by the administrator, and only from the mobile device they own. Any other connection coming from a mobile device that is not listed as a valid device for a certain user will be rejected, thus preventing fraud.

Products used for the e-Voting system

Domino Enterprise Server and Domino Everyplace

Domino Family of Servers provides a multiplatform foundation for collaboration and e-business, driving solutions from corporate messaging to Web based transactions - and everything in between. This enterprise-class messaging and collaboration system is built to maximize human productivity by unleashing the experience and expertise of individuals, teams, and extended communities.

IBM Lotus Domino Everyplace software can deliver notification of upcoming calendar events to users. Domino Everyplace software extends the capabilities of key Domino applications to supported mobile devices, providing reliable and easy-to-administer mobile and wireless services with security features.

Mobile and wireless devices, like advanced cell phones and PDAs, are becoming an accepted part of the organizations. These devices first made their way into the corporate IT infrastructure as unsupported devices purchased by individuals, for the purpose of personal productivity and organization. Over the past several years, corporations have been realizing the potential of these devices as ways to extend enterprise computing resources, to reach a new user base and provide productivity tools for the existing user base. Or they have been forced to face the task of getting these devices under control in their company.

The Domino Everyplace solution includes three key components. Domino Everyplace Access offers out-of-the-box, realtime, wireless access to Domino server-based e-mail, calendar, to-do list, contact and directory applications from microbrowser-enabled devices, such as mobile phones and PDAs. Keeping mobile and wireless users connected to their data in realtime. Domino Everyplace Short Message Service (SMS) delivers instant, efficient communication with short messaging, paging and notification services. So users can send short messages to and receive short messages from pagers and SMS component-supported mobile phones and PDAs.

Domino Everyplace Access allows users with WAP-enabled devices to access information from Domino in real time. Based on an XML architecture, Domino Everyplace Access extends the value of Domino e-collaborative services to the latest generation of WML-based microbrowser devices. As a Domino servlet, it acts as a proxy for handling communications between Domino servers and wireless devices.

Domino Everyplace Access also provides you with the possibility to create customized WAP solutions based on standard Domino applications, such as sales force automation, field service, and customer relationship management. Applications are easily deployed by use of the Domino Directory.

Domino Everyplace can associate an authorized user with each mobile device, track what network a device is used on, and encrypt data transmission. The robust Domino security features control who gets into your network and what gets out over it. Domino Everyplace Access builds on this secure environment with new standards such as Secure Sockets Layer (SSL) and Wireless Transport Layer Security (WTLS).

Security

Appropriateness of SSL/TLS to the CyberVote system

The SSL/TLS protocol provides a secure channel between a client and server entity. Data exchanged between client and server is authenticated, encrypted, and integrity-protected. However, no other security services are provided by SSL/TLS. Moreover, all cryptographic protection is only applied during transit of the data, and is removed once it is received at the other end of the secure channel.

SSL/TLS might therefore be used to implement a very basic voting system. It is much more appropriate to rely on SSL/TLS as an additional security measure besides the CyberVote voting protocols, and whenever a secure communications channel is required.

SSL/TLS is particularly suited to provide authentication of the different web servers that are involved in the voting system, e.g., servers that provide crucial guidelines to the voters, as well as servers that provide the software needed to participate in the voting process. As such, SSL/TLS can prevent that malicious parties try to masquerade as genuine voting entities.

Today’s popular browsers implement the SSL/TLS protocol by default. Netscape Communicator (4.7) only supports SSL and does not support TLS, while Netscape 6, Microsoft Internet Explorer and Opera do support both SSL and TLS. Note that in addition Microsoft also supports their own PCT 1.0 protocol.

The previously mentioned browsers all support the RC2, RC4, DES, 3DES symmetric algorithms, and MD5 and SHA-1 cryptographic hash functions. They only provide full support for RSA, while DH key establishment is not foreseen.

Note that Netscape and Opera allow the user to select preferred ciphers, while Microsoft Internet Explorer does not provide a user interface through which ciphers are configurable.

Web technologies

During the past ten years web technologies’ evolution was spectacular, along with a constant growth in number of internet users.

Due to the portability they offer, web technologies are extensively used in the enterprise businesses. Recent developments in areas of content management, network security, as well as the development of mobile devices made this kind of technologies absolutely unreplaceable in complex information systems.

The same time with the development of all of the above, the IT world felt the need for integration. Because of so many different platforms – operating systems, hardware it was sometimes difficult for large integration systems to function. That is why a new language has appeared: Java. Java is heavily used nowadays because of its multiplatform capabilities. The real integration however was achieved when a new player entered the arena: Simple Object Access Protocol – SOAP.

SOAP was first developed by Microsoft and it defines a Remote Procedure Call (RPC) mechanism using XML (eXtensible Markup Language) for client-server interaction across a network by using HTTP as the transport protocol and XML documents for encoding the messages. Using distributed object protocols on the public Internet is very problematic. Indeed, most organisations insert a firewall between their publicly accessible Web servers and the masses that can access those servers. Firewalls secure use of the Internet by blocking incoming traffic based on various criteria. In general, firewalls are configured to allow traffic on port 80 (HTTP port) so as to let HTTP requests from browsers get through, and to block most other ports, whereas distributed object protocols don't generally have a single well-know port number assigned to them. So, the utilisation of a distributed object protocols depends on the configuration of the servers. As for SOAP, it uses XML to define the format of request and response messages and then allows the use of the normal HTTP POST command to send this information. All SOAP traffic goes through port 80, which means that SOAP can be used on the Internet with any server, firewalls are no longer a problem. SOAP can take advantage of all HTTP's connection management facilities. Indeed, one of the primary design goals for SOAP is to ensure that it can be used on top of the Internet's existing infrastructure. For example SOAP can use the Secure Sockets Layer (SSL) protocol for security.